Abstract

A method and system of detecting vulnerabilities in source code. Source code is parsed into an intermediate representation. Models (e.g., in the form of lattices) are derived for the variables in the code and for the variables and/or expressions used in conjunction with routine calls. The models are then analyzed in conjunction with pre-specified rules about the routines to determine if the routine call posses one or more of pre-selected vulnerabilities.